UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

MARY MOSES Individually, and on Behalf of All Others Similarly Situated,	)	Case No.:
Plaintiff,	)	
v.	)	**JURY TRIAL DEMANDED**
SET FORTH, INC. and CENTREX SOFTWARE, INC.,	)	
Defendants.	)	

CLASS ACTION COMPLAINT

Plaintiff Mary Moses, ("Plaintiff"), through her undersigned counsel, brings this action against Set Forth, Inc. ("Forth") and Centrex Software, Inc. ("Centrex", collectively "Defendants") pursuant to the investigation of her attorney, personal knowledge as to herself and her own acts and otherwise upon information and belief, and alleges as follows:

INTRODUCTION

1. Forth is a self-described company which offers "online account administration services to consumers enrolled in debt relief programs."[1] Court filings have described it as a company that "offer[s] payment processing to debt settlement compan[ies]."[2]

2. Centrex is a software company that advertises itself as a company selling "fintech solutions that can be used to start, build, grow, and maintain your finance or fintech company."[3]

---

[1] *See* https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/5c00fedb-134a-4436-b778-5df30b84cdab.html, last accessed November 13, 2024.

[2] *RAM Payment, LLC v. Set Forth, Inc. et al.*, Case No. 2024CH04841, Cir. Ct. Cook Cty., Complaint at ¶2.

[3] https://www.centrexsoftware.com/, last accessed November 13, 2024.

In its notice of the Maine Attorney General, Forth described Centrex as a "business-to-business partner."[4] In its letter to affected persons, Centrex described itself as a provider of "cloud-based customer relationship management solutions."

3. On or about November 8, 2024, Centrex and Forth announced publicly that in or around May 2024, one or both had been the recipient of a hack and exfiltration of sensitive personal information ("SPI") involving approximately 1.5 million individuals (the "Data Breach").[5]

4. Forth and Centrex have stated that the information obtained in the hack included at least names, addresses, dates of birth, and Social Security numbers.

5. Plaintiff and Class members now face a present and imminent lifetime risk of identity theft, which is heightened here by the loss of Social Security numbers.

6. The information stolen in cyber-attacks allows the modern thief to assume your identity when carrying out criminal acts such as:

- Using your credit history.
- Making financial transactions on your behalf, including opening credit accounts in your name.
- Impersonating you via mail and/or email.
- Impersonating you in cyber forums and social networks.
- Stealing benefits that belong to you.
- Committing illegal acts which, in turn, incriminate you.

7. Plaintiff's and Class members' SPI was compromised due to Defendant's negligent and/or careless acts and omissions and the failure to protect the SPI of Plaintiff and Class members.

---

[4] *See* https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/5c00fedb-134a-4436-b778-5df30b84cdab.html, last accessed November 13, 2024.

[5] *Id.*

8. As of this writing, there exist many class members who have no idea their SPI has been compromised, and that they are at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

9. Plaintiff brings this action on behalf of all persons whose SPI was compromised as a result of Defendants' failure to: (i) adequately protect individuals' SPI, (ii) adequately warn these individuals of its inadequate information security practices, and (iii) effectively monitor its platforms for security vulnerabilities and incidents (the "Class"). Defendants' conduct amounts to negligence and violates federal and state statutes.

10. Plaintiff and similarly situated individuals have suffered injury as a result of Defendant's conduct. These injuries include: (i) lost or diminished inherent value of SPI; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their SPI; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iv) deprivation of rights they possess under state and common law; and (v) the continued and certainly an increased risk to their SPI, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the SPI.

JURISDICTION AND VENUE

11. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendants.

12. This Court has personal jurisdiction over Defendants because Defendant Forth's principal place of business is located within this District.

13. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because a substantial

part of the events or omissions giving rise to these claims occurred in, were directed to, and/or emanated from this District. Defendant Forth resides within this judicial district and a substantial part of the events giving rise to the claims alleged herein occurred within this judicial district.

PARTIES

14. Plaintiff Mary Moses is a natural person residing in Wise County, Virginia. On or about November 13, 2024, Plaintiff was informed via letter dated November 8, 2024 that she had been a victim of the Data Breach.

15. Defendant Set Forth, Inc. is a Delaware corporation with its principal place of business at 1900 E. Golf Road, Suite 550, Schaumburg, Illinois.

16. Defendant Centrex Software, Inc. is a California corporation with its principal place of business at 3090 Pullman Street Suite F, Costa Mesa, California.

FACTUAL ALLEGATIONS

17. As stated above, Forth is a company that specializes in collecting and administering the SPI of individuals, though how it acquires or maintains that SPI is not entirely clear.

18. Centrex is a software company that provides or licenses its software to financial services companies, including Forth.

19. In the ordinary course of doing business, Defendants collect SPI such as:

a. Contact information, such as names, addresses, telephone numbers, email addresses, and household members;

b. Authentication and security information such as government identification, Social Security number, driver's license number; and

c. Demographic information, such as age, gender, and date of birth;

20. It is unclear how Defendants acquire this information, and Defendants do not make it clear from their notice letters or, in Centrex's case, its website, how it acquires this information.

21. Forth indicates from its letter to the Maine Attorney General that it has a "business-to-business" relationship with Centrex and that affected individuals "may be receiving this letter if you were a customer or have done business with Centrex, Inc."[6]

22. Centrex, by contrast, states in its notice letter that it "provides cloud-based customer relationship management (CRM) solutions powered by the Set Forth platform." It further states that it "allows businesses to collect and share consumer information, with their permission, between its users."

23. Whose permission is required to share information is not clear, and Plaintiff is unaware of having ever given her permission for either Forth or Centrex to acquire or share her SPI.

24. Centrex includes a Privacy Policy on its website. The Privacy Policy includes the following representation:

> [Centrex] collects and uses your personal information to operate its website(s) and deliver the services you have requested.
>
> . . .
>
> CTX will disclose your personal information, without notice, only if required to do so by law or in the good faith belief that such action is necessary to: (a) conform to the edicts of the law or comply with legal process served on CTX or the site; (b) protect and defend the rights or property of CTX; and, (c) act under exigent circumstances to protect the personal safety of users of CTX, or the public.
>
> CTX will retain your personal information for the length of time needed to fulfill the purposes outlined in this privacy policy unless a longer retention period is required or permitted by law.[7]

---

[6] *Id.*

[7] https://www.centrexsoftware.com/privacy-policy/, last accessed November 14, 2024.

25. Defendant Forth does not appear to maintain a website, much less a privacy policy.

26. On or about November 8, 2024, Defendants announced publicly that on or about May 21, 2024, both became aware of a hack and exfiltration of sensitive personal information involving affected persons.[8]

27. The notice provided by Forth to the Maine Attorney General states that "On May 21, 2024, Forth identified suspicious activity on its system, and immediately implemented our incident response protocols, and engaged independent computer forensic specialists to investigate the activity and determine what, if any, data may have been impacted. The investigation determined that personal information belonging to yourself, a spouse, co-applicant, or dependent may have been accessed during the incident."[9]

28. By contrast, the letter sent by Centrex states, "In May 2024, Centrex identified suspicious activity on the network. We immediately implemented our incident response protocols, took steps to secure the network, and engaged independent computer forensic experts to assist us in conducting an investigation. Unfortunately, the investigation determined that business documents (such as loan applications, credit reports, and bank statements) that may have contained personal information belonging to you, your spouse, a co-applicant, or a dependent may have been accessed during the incident."

29. Forth reported to the Maine Attorney General that the Data Breach affected approximately 1.5 million individuals.[10]

---

[8] *See* https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/5c00fedb-134a-4436-b778-5df30b84cdab.html, last accessed November 13, 2024.
[9] *Id*.
[10] *Id.*

30. As a result, Plaintiff's and class members' SPI was in the hands of hackers for at least five months before Defendants began notifying them of the Data Breach.

31. Defendants have been vague on its response to the Data Breach, with Forth stating only that "We want to assure you that we are taking steps to prevent a similar incident from happening in the future. Since the incident, we deployed enhanced endpoint monitoring software, performed a global password reset, and implemented additional security controls."[11]

32. As of this writing, Defendants have offered no concrete information on the steps it has taken or specific efforts made to reasonably ensure that such a breach cannot or will not occur again.

33. Defendanta have also stated that it they are offering credit monitoring for twelve months to impacted individuals.

34. However, this response is entirely inadequate to Plaintiff and class members who now potentially face several years of heightened risk from the theft of their SPI and who may have already incurred substantial out-of-pocket costs in responding to the Data Breach.

35. Defendants had obligations created by contract, industry standards, common law, and representations made to Plaintiff and Class members, to keep their SPI confidential and to protect it from unauthorized access and disclosure.

36. Plaintiff and Class members provided their SPI to Defendants with the reasonable expectation and mutual understanding that Defendants would comply with its obligations to keep such information confidential and secure from unauthorized access.

37. Defendants' data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches in the cellular communications services

---

[11] *Id.*

industry preceding the date of the breach.

38. Indeed, data breaches, such as the one experienced by Defendants, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known and completely foreseeable to the public and to anyone in Defendants' industry, including Defendants.

39. According to the Federal Trade Commission ("FTC"), identity theft wreaks havoc on consumers' finances, credit history, and reputation and can take time, money, and patience to resolve.[12] Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank and finance fraud.[13]

40. The SPI of Plaintiff and members of the Classes was taken by hackers to engage in identity theft or and or to sell it to other criminals who will purchase the SPI for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

41. Defendants knew, or reasonably should have known, of the importance of safeguarding the SPI of Plaintiff and members of the Class, including Social Security numbers, driver license or state identification numbers, and/or dates of birth, and of the foreseeable consequences that would occur if Defendants' data security systems were breached, including, specifically, the significant costs that would be imposed on Plaintiff and members of the Class a result of a breach.

42. Plaintiff and members of the Class now face years of constant surveillance of their

---

[12] *See Taking Charge, What to Do If Your Identity is Stolen*, FTC, 3 (Apr. 2013), https://dss.mo.gov/cd/older-youth-program/files/taking-charge-what-to-do-if-identity-is-stolen.pdf, last accessed November 14, 2024.

[13] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 CFR § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." *Id*.

financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their SPI.

43. The injuries to Plaintiff and members of the Class were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the SPI of Plaintiff and members of the Class.

44. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

45. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their networks' vulnerabilities; and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

46. The FTC further recommends that companies not maintain SPI longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

47. The FTC has brought enforcement actions against businesses for failing to protect consumer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take

to meet their data security obligations.

48. Defendants failed to properly implement basic data security practices, and its failure to employ reasonable and appropriate measures to protect against unauthorized access to student and applicant SPI constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

49. A number of industry and national best practices have been published and should have been used as a go-to resource and authoritative guide when developing Defendant's cybersecurity practices.

50. Best cybersecurity practices include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

51. Upon information and belief, Defendants failed to meet the minimum standards of the following cybersecurity frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established standards in reasonable cybersecurity readiness.

52. These foregoing frameworks are existing and applicable industry standards in Defendants' industry, and Defendants failed to comply with these accepted standards, thereby opening the door to the cyber-attack and causing the Data Breach.

53. Businesses that store personal information are likely to be targeted by cyber criminals. Credit card and bank account numbers are tempting targets for hackers. However, information such as dates of birth and Social Security numbers are even more attractive to hackers; they are not easily destroyed and can be easily used to perpetrate identity theft and other types of fraud.

54. The SPI of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[14]

55. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration ("SSA") stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[15]

56. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

57. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited

---

[14] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs, last accessed November 14, 2024.

[15] SSA, *Identity Theft and Your Social Security Number*, SSA Publication No. 05-10064 (Jun. 2018), https://www.ssa.gov/pubs/EN-05-10064.pdf, last accessed November 14, 2024.

into the new Social Security number."[16]

58. Furthermore, as the SSA warns:

> Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.
>
> If you receive a new Social Security Number, you should not be able to use the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under the new number may make more difficult for you to get credit.[17]

59. Here, the unauthorized access left the cyber criminals with the tools to perform the most thorough identity theft—they have obtained all the essential SPI to mimic the identity of the user. The personal data of Plaintiff and members of the Class stolen in the Data Breach constitutes a dream for hackers and a nightmare for Plaintiff and the Class. Stolen personal data of Plaintiff and members of the Classes represents essentially one-stop shopping for identity thieves.

60. The FTC has released its updated publication on protecting SPI for businesses, which includes instructions on protecting SPI, properly disposing of SPI, understanding network vulnerabilities, implementing policies to correct security problems, using intrusion detection programs, monitoring data traffic, and having in place a response plan.

61. General policy reasons support such an approach. A person whose personal information has been compromised may not see any signs of identity theft for years. According to the United States Government Accountability Office ("GAO") Report to Congressional

---

[16] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft, last accessed November 14, 2024.

[17] SSA, *Identity Theft and Your Social Security Number*, SSA Publication No. 05-10064 (Jun. 2018), http://www.ssa.gov/pubs/EN-05-10064.pdf, last accessed November 14, 2024.

Requesters:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[18]

62. Companies recognize that SPI is a valuable asset. Indeed, SPI is a valuable commodity. A "cyber black-market" exists in which criminals openly post stolen Social Security numbers and other SPI on a number of Internet websites. The stolen personal data of Plaintiff and members of the Class has a high value on both legitimate and black markets.

63. Identity thieves may commit various types of crimes such as immigration fraud, obtaining a driver license or identification card in the victim's name but with another's picture, and/or using the victim's information to obtain a fraudulent tax refund or fraudulent unemployment benefits. The United States government and privacy experts acknowledge that it may take years for identity theft to come to light and be detected.

64. As noted above, the disclosure of Social Security numbers in particular poses a significant risk. Criminals can, for example, use Social Security numbers to create false bank accounts or file fraudulent tax returns. Defendant's former and current customers whose Social Security numbers have been compromised now face a real, present, imminent and substantial risk of identity theft and other problems associated with the disclosure of their Social Security number and will need to monitor their credit and tax filings for an indefinite duration.

65. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change — Social Security number, driver license number or government-issued identification number,

---

[18] *See* https://www.gao.gov/assets/gao-07-737.pdf (June 2007) at 29, last accessed November 14, 2024.

name, and date of birth.

66. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[19]

67. Among other forms of fraud, identity thieves may obtain driver licenses, government benefits, medical services, and housing or even give false information to police. An individual may not know that his or her driver license was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud, or until the individual attempts to lawfully apply for unemployment and is denied benefits (due to the prior, fraudulent application and award of benefits)

FACTS SPECIFIC TO PLAINTIFF

68. On or about November 13, 2024, Plaintiff was notified via letter from Defendant Centrex dated November 8, 2024 that Plaintiff's SPI had been taken as part of the Data Breach.

69. Plaintiff has no knowledge of how Defendants acquired Plaintiff's SPI.

70. Plaintiff has spent considerable time dealing with the fallout from the breach.

71. Further, Plaintiff has experienced anxiety, emotional distress, and increased concerns for the loss of her privacy since the time of the breach.

72. Plaintiff is aware of no other source from which the theft of her SPI could have come. He regularly takes steps to safeguard her SPI in her own control.

---

[19] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed July 15, 2022)

CLASS ACTION ALLEGATIONS

73. Plaintiff brings this nationwide class action, pursuant to Rules 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure, on behalf of all members of the following class:

> All natural persons residing in the United States whose SPI was compromised in the Data Breach announced by Defendants on or about November 8, 2024 (the "Nationwide Class" or "the Class").

74. Excluded from the Class are all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out, and all judges assigned to hear any aspect of this litigation and their immediate family members.

75. Plaintiff reserves the right to modify or amend the definitions of the proposed Class before the Court determines whether certification is appropriate.

76. **Numerosity**: The Class and Subclass are so numerous that joinder of all members is impracticable. Defendant Forth has, as of this writing, indicated to the Maine Attorney General that the total number of Class Members is approximately 1.5 milion. The Class is readily identifiable within Defendants' records.

77. **Commonality**: Questions of law and fact common to the Class and Subclass exist and predominate over any questions affecting only individual members of the Class and Subclass These include:

a. When Defendants actually learned of the Data Breach and whether its response was adequate;

b. Whether Defendants owed a duty to the Class and Subclass to exercise due care in collecting, storing, safeguarding and/or obtaining their SPI;

c. Whether Defendants breached that duty;

d. Whether Defendants implemented and maintained reasonable security procedures and practices appropriate to the nature of storing the SPI of Plaintiff and members of the Class;

e. Whether Defendants acted negligently in connection with the monitoring and/or

protection of SPI belonging to Plaintiff and members of the Class and Subclass;

f. Whether Defendants knew or should have known that it did not employ reasonable measures to keep the SPI of Plaintiff and members of the Class and Subclass secure and to prevent loss or misuse of that SPI;

g. Whether Defendants have adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

h. Whether Defendants caused Plaintiff and members of the Class and Subclass damage;

i. Whether Defendants violated the law by failing to promptly notify Plaintiff and members of the Class and Subclass that their SPI had been compromised; and

j. Whether Plaintiff and the other members of the Class and Subclass are entitled to credit monitoring and other monetary relief.

78. **Typicality**: Plaintiff's claims are typical of those of the other members of the Class and Subclass because all had their SPI compromised as a result of the Data Breach due to Defendants' misfeasance.

79. **Adequacy**: Plaintiff will fairly and adequately represent and protect the interests of the members of the Class and Subclass. Plaintiff's counsel are competent and experienced in litigating privacy-related class actions.

80. **Superiority and Manageability**: Under rule 23(b)(3) of the Federal Rules of Civil Procedure, a class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all the members of the Class and Subclass are impracticable. Individual damages for any individual member of the Class and Subclass are likely to be insufficient to justify the cost of individual litigation, so that in the absence of class treatment, Defendants' misconduct would go unpunished. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action.

81. Class certification is also appropriate under Rule 23(a) and (b)(2) because Defendants have acted or refused to act on grounds generally applicable to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Class.

82. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendants owed a legal duty to Plaintiff and members of the Class and to exercise due care in collecting, storing, using, and safeguarding their SPI;

b. Whether Defendants breached a legal duty to Plaintiff and the members of the Class to exercise due care in collecting, storing, using, and safeguarding their SPI;

c. Whether Defendants failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach; and

e. Whether members of the Class are entitled to actual damages, credit monitoring or other injunctive relief, and/or punitive damages as a result of Defendants' wrongful conduct.

FIRST CLAIM FOR RELIEF
Negligence
(By Plaintiff Individually and on Behalf of the Class)

83. Plaintiff hereby re-alleges and incorporates by reference all of the allegations in paragraphs 1 to 82.

84. Defendants appear to routinely handle SPI that is required of their customers, which includes the SPI of Plaintiff and members of the Class.

85. By collecting and storing the SPI of its customers, Defendants owed a duty of care

to the individuals whose SPI it collected to use reasonable means to secure and safeguard that SPI.

86. As companies that work in financial technology, Defendants are aware of that duty of care to the SPI.

87. Defendants have full knowledge of the sensitivity of the SPI and the types of harm that Plaintiff and Class Members could and would suffer if the SPI were wrongfully disclosed.

88. Defendants knew or reasonably should have known that its failure to exercise due care in the collecting, storing, and using of this SPI involved an unreasonable risk of harm to Plaintiff and Class Members, even if the harm occurred through the criminal acts of a third party.

89. Defendants had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendants' security protocols to ensure that Plaintiff's and Class Members' information in Defendants' possession was adequately secured and protected.

90. Defendants also had a duty to have procedures in place to detect and prevent the improper access and misuse of Plaintiff's and Class Members' SPI.

91. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class Members was reasonably foreseeable, particularly in light of Defendants' inadequate security practices.

92. Plaintiff and the Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Defendants knew of should have known of the inherent risks in collecting and storing the SPI of Plaintiff and the Class, the critical importance of providing adequate security of that SPI, and the necessity for encrypting SPI stored on Defendants' systems.

93. Defendants' own conduct created a foreseeable risk of harm to Plaintiff and Class Members. Defendants' misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendants' misconduct also included its decisions not to comply with industry standards for the safekeeping of Plaintiff's and

Class Members' SPI, including basic encryption techniques freely available to Defendants.

94. As a sophisticated web-based company that routinely handles sensitive information, Defendants had a duty of care to Plaintiff and Class Members.

95. Plaintiff and the Class Members had no ability to protect their SPI that was in, and possibly remains in, Defendants' possession.

96. Defendants were in a position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

97. Defendants had and continue to have a duty to adequately disclose that the SPI of Plaintiff and Class Members within Defendants' possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Class Members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their SPI by third parties.

98. Defendants had a duty to employ proper procedures to prevent the unauthorized dissemination of the SPI of Plaintiff and Class Members.

99. Defendants have admitted that the SPI of Plaintiff and Class Members was purposely exfiltrated and disclosed to unauthorized third persons as a result of the Data Breach.

100. Defendants, through their actions and/or omissions, unlawfully breached its duties to Plaintiff and Class Members by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the SPI of Plaintiff and Class Members during the time the SPI was within Defendants' possession or control.

101. Defendants improperly and inadequately safeguarded the SPI of Plaintiff and Class Members in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

102. Defendants failed to heed industry warnings and alerts to provide adequate safeguards to protect the SPI it had in its possession in the face of increased risk of theft.

103. Defendants, through their actions and/or omissions, unlawfully breached their duty to Plaintiff and Class Members by failing to have appropriate procedures in place to detect and

prevent dissemination of the SPI in question.

104. Defendants, through their actions and/or omissions, unlawfully breached their duty to adequately and timely disclose to Plaintiff and Class Members the existence and scope of the Data Breach.

105. But for Defendants' wrongful and negligent breach of duties owed to Plaintiff and Class Members, the SPI of Plaintiff and Class Members would not have been compromised.

106. There is a close causal connection between Defendants' failure to implement security measures to protect the SPI of Plaintiff and Class Members and the harm suffered or risk of imminent harm suffered by Plaintiff and the Class. Plaintiff's and Class Members' SPI was lost and accessed as the proximate result of Defendants' failure to exercise reasonable care in safeguarding such SPI by adopting, implementing, and maintaining appropriate security measures.

107. Given Defendants' sophistication in the provision of online services and the potential likelihood of injury should it fail in its duties, the burden on Defendants to properly safeguard Plaintiff's and Class Members' SPI would be relatively light.

108. As a direct and proximate result of Defendants' negligence, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their SPI is used; (iii) the compromise, publication, and/or theft of their SPI; (iv) damages for emotional distress and anxiety; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) the continued risk to their SPI, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fails to undertake appropriate and adequate measures to protect the SPI of its employees and former employees in its possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the SPI compromised as a result of the Data Breach for the remainder of Plaintiff's and Class Members' lives.

109. Additionally, as a direct and proximate result of Defendants' negligence, Plaintiff and Class Members have suffered and will continue to suffer anxiety and emotional distress, and well as suffering the continued risks of exposure of their SPI, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the SPI in its continued possession.

SECOND CLAIM FOR RELIEF
Breach of Third-Party Beneficiary Contract,
(By Plaintiff Individually and on Behalf of the Class)

110. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 82.

111. Upon information and belief, Defendants entered into contracts with their corporate customers to provide services to them; services that included data security practices, procedures, and protocols sufficient to safeguard the SPI that was entrusted to them.

112. Such contracts were made expressly for the benefit of Plaintiff and the Class, as it was their SPI that Defendants agreed to receive, store, utilize, transfer, and protect through its services. Thus, the benefit of collection and protection of the SPI belonging to Plaintiff and the Class was the direct and primary objective of the contracting parties and Plaintiff and Class Members were direct and express beneficiaries of such contracts.

113. Defendants knew or should have known that if they were to breach these contracts with its customers, Plaintiff and Class Members would be harmed.

114. Defendants breached their contracts with corporate customers by, among other things, failing to adequately secure Plaintiff and Class Members' SPI, and, as a result, Plaintiff and Class Members were harmed by Defendants' failure to secure their SPI.

115. As a direct and proximate result of Defendants' breach, Plaintiff and Class Members are at a current and ongoing risk of identity theft, and Plaintiff and Class Members sustained incidental and consequential damages including: (i) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (ii) loss of time and

loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (iii) financial "out of pocket" costs incurred due to actual identity theft; (iv) loss of time incurred due to actual identity theft; (v) loss of time due to increased spam and targeted marketing emails; (vi) diminution of value of their SPI; (vii) future costs of identity theft monitoring; (viii) and the continued risk to their SPI, which remains in Defendants' control, and which is subject to further breaches, so long as Defendants fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' SPI.

116. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

117. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendants to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

THIRD CLAIM FOR RELIEF
Unjust Enrichment, in the Alternative
(By Plaintiff Individually and on Behalf of the Class)

118. Plaintiff hereby re-alleges and incorporates by reference all of the allegations in paragraphs 1 to 82.

119. Plaintiff and Class Members conferred a monetary benefit upon Defendants in the form of storing their SPI with in such a way that saved expense and labor for Defendants.

120. Defendants appreciated or had knowledge of the benefits conferred upon it by Plaintiff and Class Members. Defendants also benefited from the receipt of Plaintiff's and Class Members' SPI, as this was used by Defendants to facilitate its core functions.

121. The benefits given by Plaintiff and Class Members to Defendants were to be used by Defendants, in part, to pay for or recoup the administrative costs of reasonable data privacy and security practices and procedures.

122. As a result of Defendants 'conduct, Plaintiff and Class Members suffered actual

damages in an amount to be determined at trial.

123. Under principles of equity and good conscience, Defendants should not be permitted to retain a benefit belonging to Plaintiff and Class Members because Defendants failed to implement (or adequately implement) the data privacy and security practices and procedures that Plaintiff and Class Members granted to Defendants or were otherwise mandated by federal, state, and local laws and industry standards.

124. Defendants should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds or benefits it received as a result of the conduct alleged herein.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and all Class Members, requests judgment against the Defendants and the following:

A. For an Order certifying the Class as defined herein, and appointing Plaintiff and their counsel to represent the Class;

B. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and the Class Members' SPI;

C. For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;

D. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

E. For pre- and postjudgment interest on all amounts awarded; and

F. Such other and further relief as this Court may deem just and proper.

JURY DEMAND

Plaintiff hereby demands a trial by jury on all issues so triable.

NOTICE TO ILLINOIS ATTORNEY GENERAL OF ACTION

Pursuant to 815 ILCS 505/10a (d), a copy of this Complaint has been mailed to the Illinois Attorney General with the filing of this Complaint.

DATED: November 15, 2024

Respectfully Submitted,

By: /s/ *Carl V. Malmstrom*
Carl V. Malmstrom
WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLC
111 W. Jackson Blvd., Suite 1700
Chicago, Illinois 60604
Tel: (312) 984-0000
Fax: (212) 686-0114
malmstrom@whafh.com

Attorney for Plaintiff and the Proposed Class